

Introducing the IANA Functions to the LAC region

Kim Davies
VP, IANA Services; President, PTI

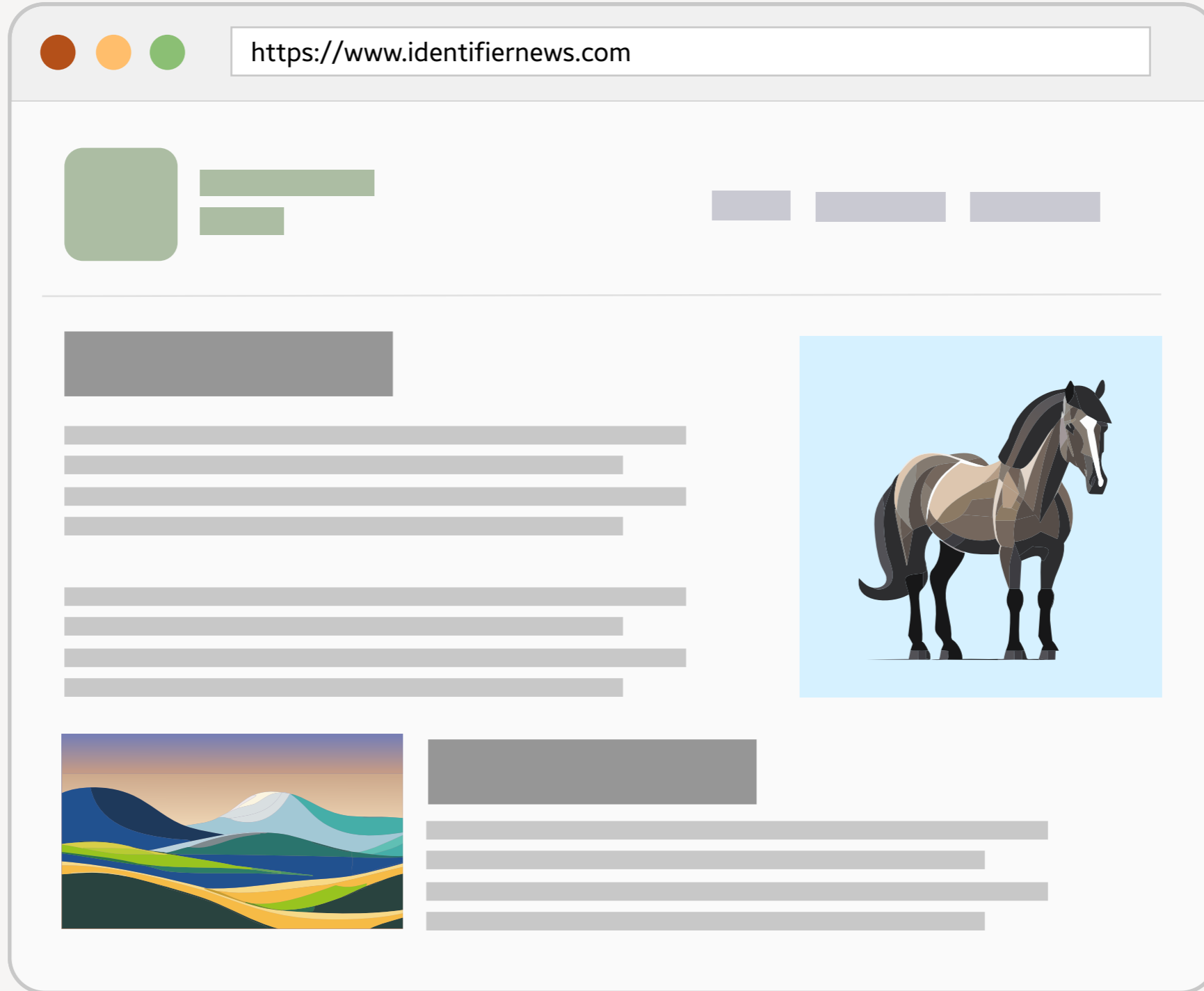
September 2024

PTI | An ICANN Affiliate



Unique identifiers

- Unique identifiers are at the heart of everything IANA, and our broader ICANN ecosystem, does.
- Let's talk about what unique identifiers are and the role they play.







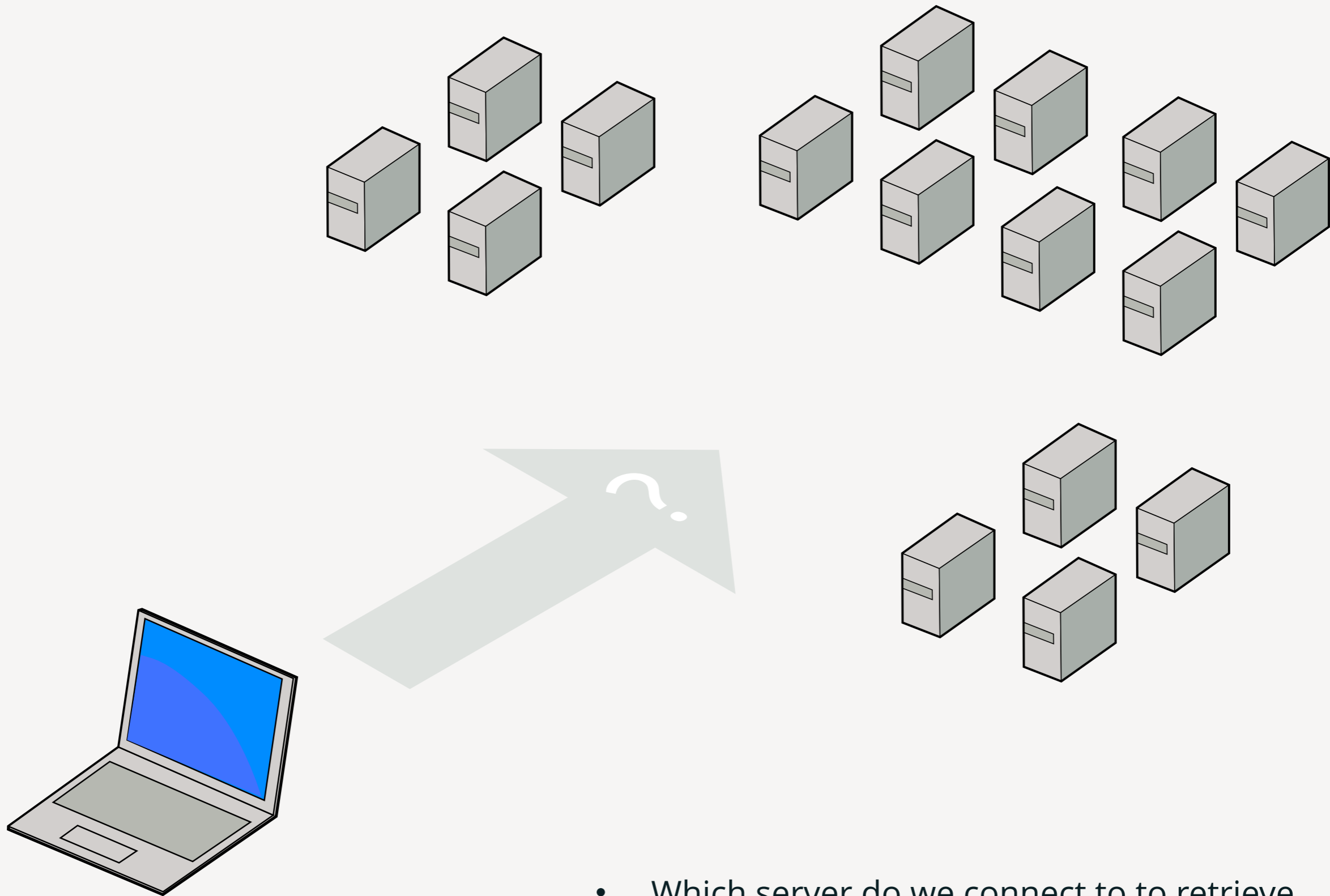
<https://identifiernews.com>

- `identifiernews.com` is a **domain name**, a human-readable address that provides a memorable means to communicate a location on the Internet.
- It forms part of a Uniform Resource Locator (URL), a common way of describing the location for something on the Internet.
- We use domain names every day for website locations, as a part of email addresses, and more.

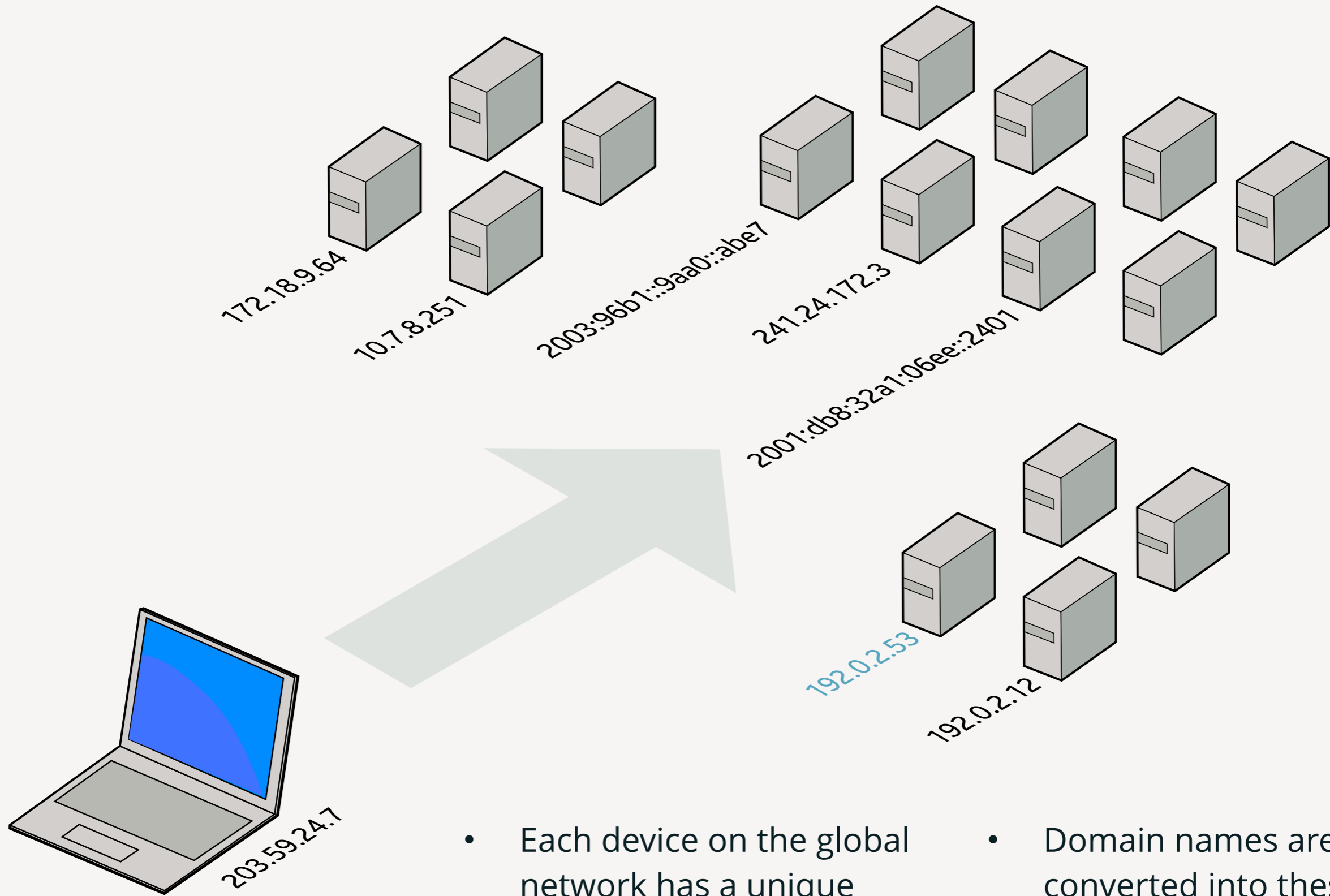


<https://identifiernews.com>

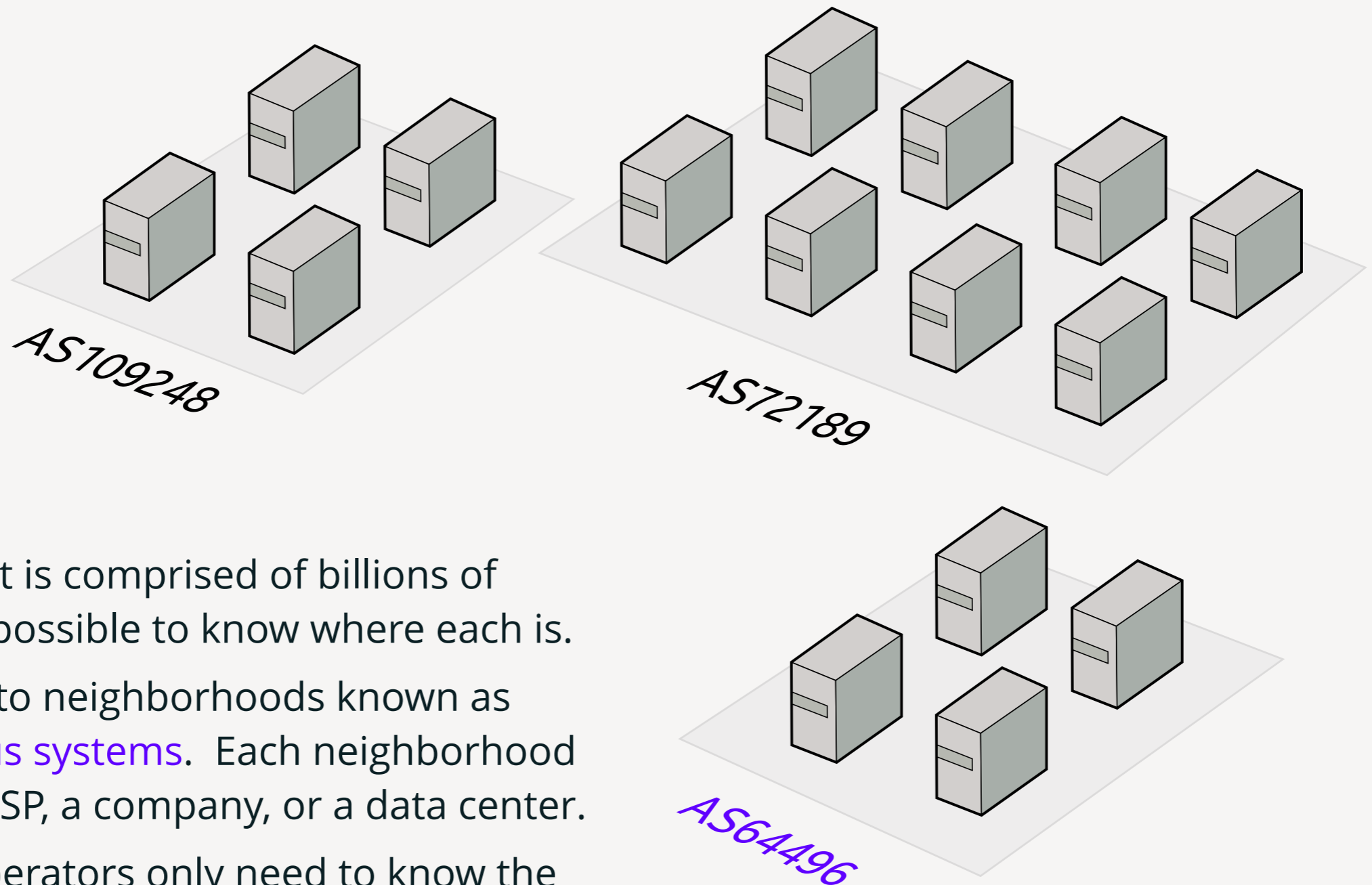
- In a URL, how do we know what type of transmission is needed to get to the location?
- `https` is another part of the URL that signals the transmission method used to reach the location, known as a **URI scheme**.
- `https` is short for for Secure Hypertext Transmission Protocol, the standard way we transmit web pages in an encrypted manner
- There are others, like `http` for non-encrypted web pages, and `ftp` for File Transfer Protocol, or `rtsp` for Realtime Streaming Protocol.
- There are over 100 URI schemes.



- Which server do we connect to to retrieve the data we want on the Internet?

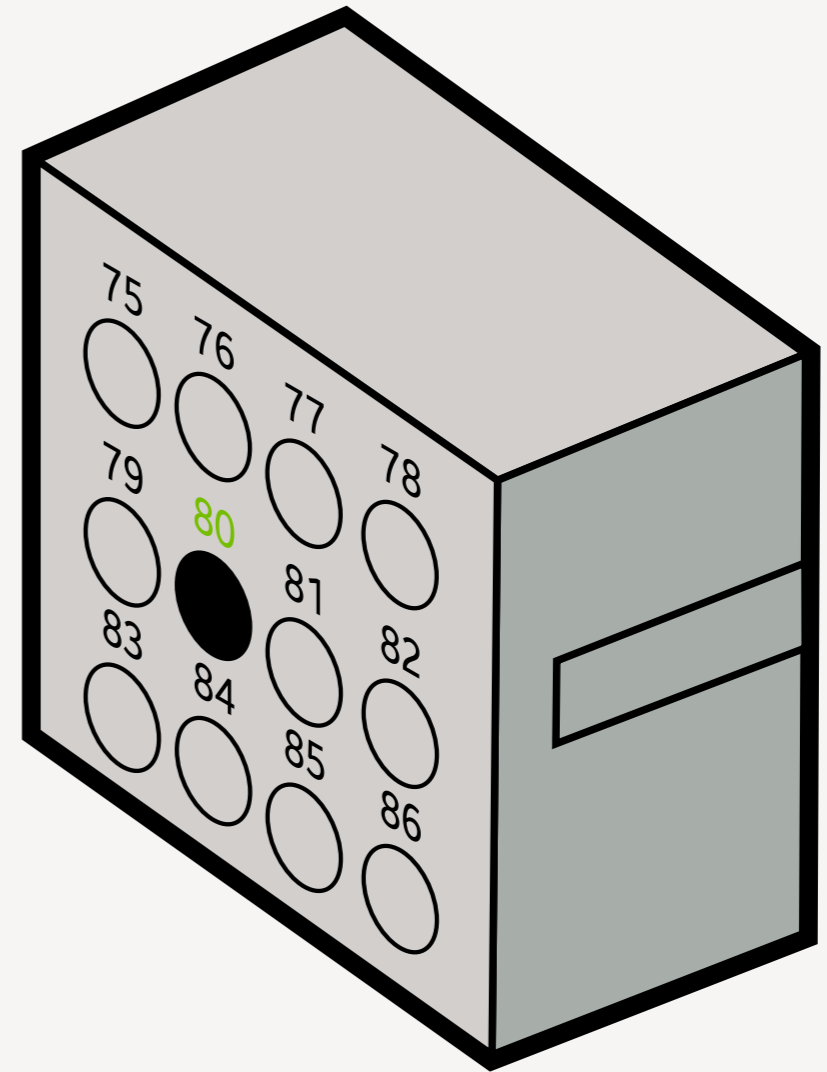


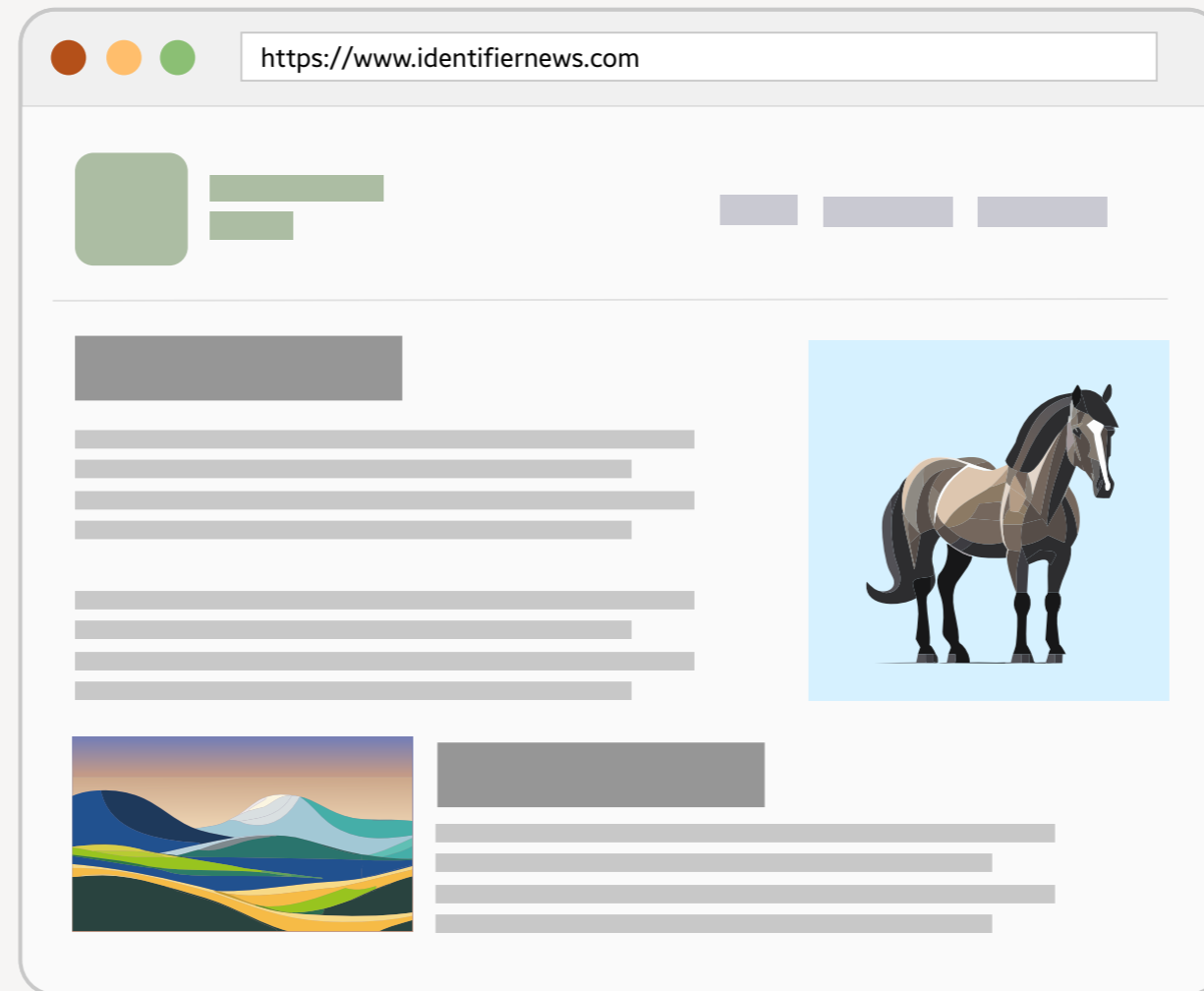
- Each device on the global network has a unique numerical identifier, called an **IP address**.
- Domain names are converted into these endpoint identifiers.



- The Internet is comprised of billions of devices, impossible to know where each is.
- Grouped into neighborhoods known as **autonomous systems**. Each neighborhood may be an ISP, a company, or a data center.
- Network operators only need to know the most efficient path between ASs without needing to know the location of each device.
- Only track the exact connection for each device in their own network.

- Individual servers on the Internet often have multiple functions: serving websites, receiving email, offering file shares, running VPNs, hosting databases.
- Each service is defined with a port, so a network connection is made to the specific port related to the type of connection you want to establish. Services available are denoted by a **service name**, and usually a unique **port number**.
- When you're requesting a web page you may connect to port 80 (for web servers), rather than 25 (for email transmission)

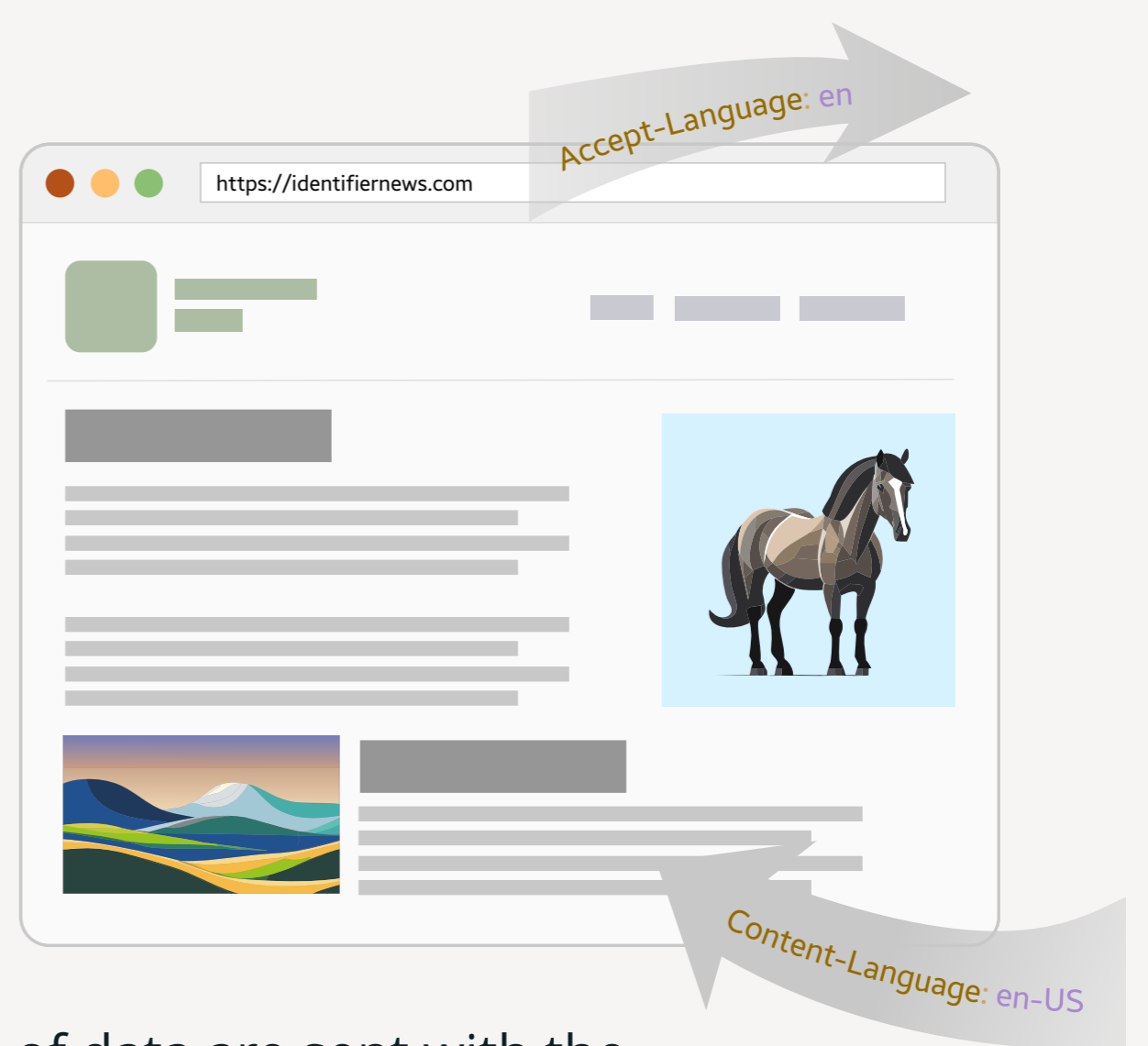




- Our device connects to a server based on an IP address and port number, and gets back web page data.
- Web pages are comprised of lots of different types of data — text, graphics, movies, interactive elements. How does a recipient know the different possible encodings to make sense of it?



- Each piece of the transmission is coded with a **media type** which ties it to the underlying format. For example, video streaming may be `video/h264`, but a static photograph would be `image/jpeg`, wrapped in text defined with `text/html` and interactive elements coded in with `application/javascript`



- When requesting a web page, additional bits of data are sent with the request to signal preferences and abilities of the web browser. These are denoted with **header fields**.
- One such field `Accept-Language`, signals language preference, so a website available in multiple languages will come back in the preferred language.
- Language choice is encoded using **language tags**. For example, `en` means English, and `en-US` means specifically American English.

Unique identifiers are everywhere

- You've now received your web page, and think about how all these unique identifiers were involved:
 - The **domain name** - the human-friendly address of the website;
 - The **URI scheme** - that tells your computer the language (protocol) it needs to speak to request the website;
 - The **IP address** - the machine-readable identifier of the server the web site is located at;
 - The **AS number** - the neighborhood the server is located in where your ISP needs to send your request to;
 - The **service name** and **port number** - that tells you which door to knock on at the server;
 - The **media type** - which helps your computer decode the data it gets back into pieces it can understand and represent on your screen;
 - The **header field** specifies extra data for requests and responses; and
 - A **language tag** signals the language desired, available and sent.

What do these all have in common?

- All of these unique identifiers are just a fraction of those necessary to transmit a single webpage across the Internet.
- Coordinating the Internet unique identifier systems is needed to ensure the Internet interoperates globally.
- If any one of those identifier types didn't have a common standardized meaning around the world, the web page would have failed to transmit across the Internet.
- **The IANA functions' responsibility is to manage all those identifiers globally.**
- This example only highlights 9 of around 3,500 identifier types managed by IANA.

32 bits

Version (1 byte)

My Autonomous System (2 bytes)

BGP Identifier (4)

Opt Param Len (1 byte)

service	proto	name	TTL	class	priority	weight	port	target
_sip._tls.example		yourdomain.com	600	IN	SRV	0	5060	sipserver.yourdomain.com

```
<RDF:Description RDF:about="urn:mimetype:image/pcl"
  NC:value="image/pcl"
  NC:editable="true"
  NC:fileExtensions="pdf"
  NC:description="Adobe Acrobat Document" >
  <NC:handlerProp RDF:resource="urn:mimetype:handler:image/pcl"/>
  <RDF:Description
    RDF:about="urn:mimetype:application/pdf"
    NC:value="application/pdf"
    Prop RDF:resource="urn:mimetype:handler:application/pdf"/>
  <RDF:Description
    RDF:about="urn:mimetype:application/atomsvc+xml"
    NC:value="application/atomsvc+xml" >
```

TCP Connection Establishment

A → B: Send SYN (1) (SEQ=100 CTL=SYN)

B → A: SYN received (2) Send SYN, ACK (SEQ=300 ACK=101 CTL=SYN, ACK)

A → B: Established (3) (SEQ=101 ACK=301 CTL=ACK)

CTL = Which control bits in the TCP header are set to 1
A sends ACK response to B.

4XX Client Error Codes
409 Conflict
410 Gone
411 Length Required
412 Precondition Failed
413 Payload Too Large
414 Request-URI Too Large
415 Unsupported Media Type
416 Requested Range Not Satisfiable
417 Expectation Failed
418 I'm a teapot
421 Misdirected Request
422 Unprocessable Entity
423 Locked
424 Failed Dependency
426 Upgrade Required
428 Precondition Required
429 Too Many Requests

3XX Redirection Codes
300 Multiple Choices
301 Moved Permanently
302 Found
303 See Other
304 Not Modified
305 Use Proxy
307 Temporary Redirect
308 Permanent Redirect

5XX Server Error Codes
500 Internal Server Error
501 Not Implemented
502 Bad Gateway
503 Service Unavailable
504 Gateway Timeout
505 HTTP Version Not Supported

Transmission Control Protocol (TCP) Header
20-60 bytes

source port number	destination port number
2 bytes	2 bytes

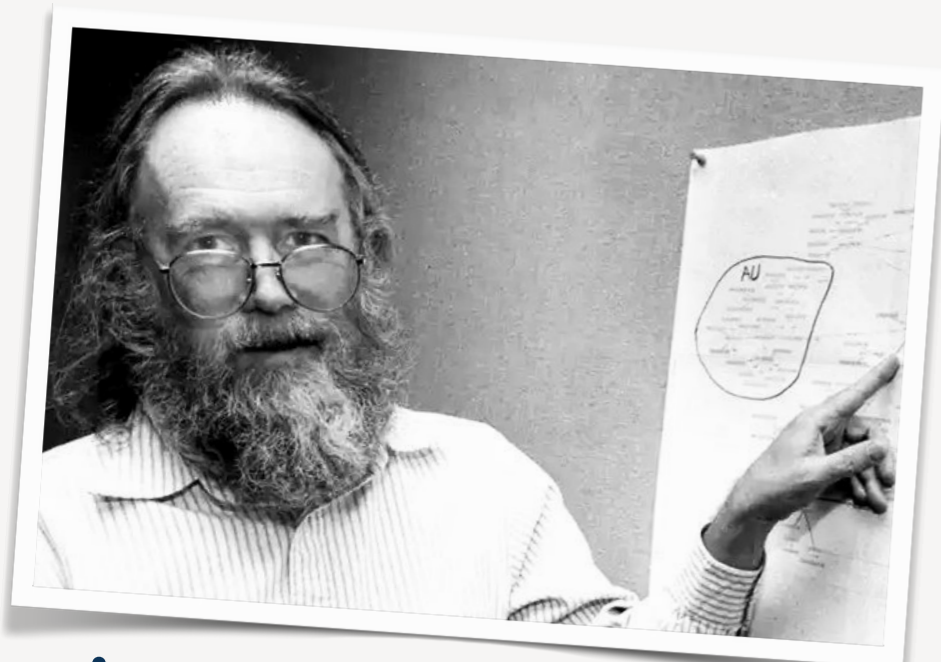
sequence number	acknowledgement number
4 bytes	4 bytes

data offset	reserved	control flags	checksum	window size	urgent pointer
4 bits	3 bits	9 bits	2 bytes	2 bytes	2 bytes

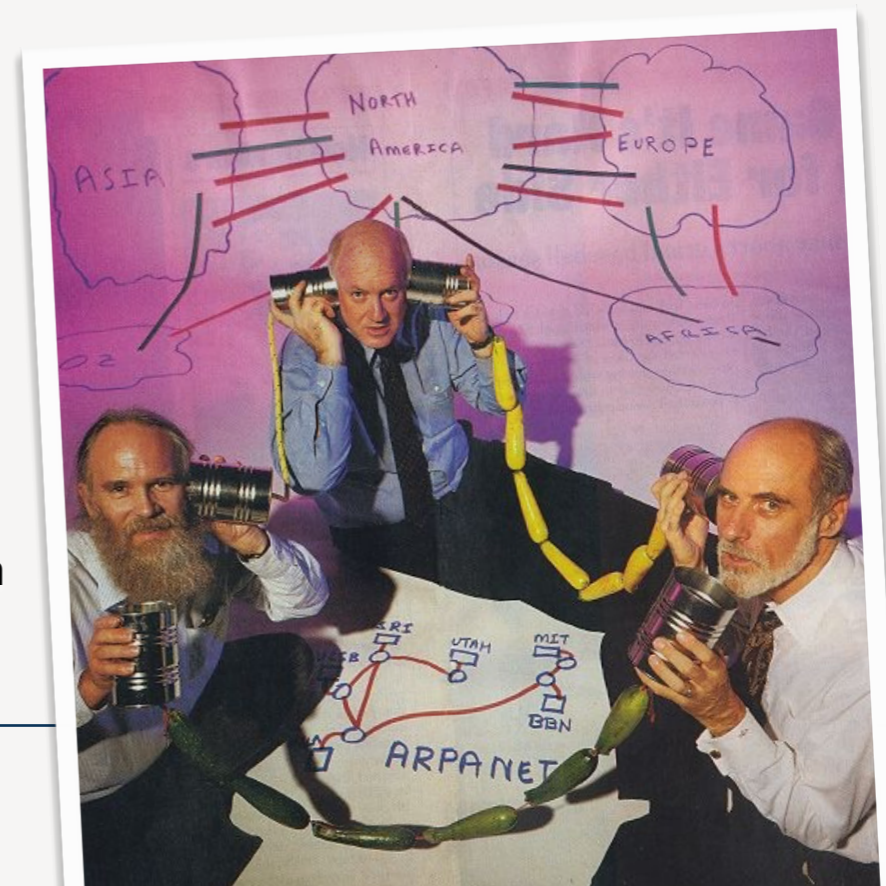
CANN Affiliate

The IANA functions

- The record keeper for the unique names and numbers used by Internet technologies to interoperate.
- The IANA functions pre-date ICANN. In 1998, ICANN was established to be the home of the IANA functions with global oversight.
- The IANA team maintains these records according to policies established in standards organizations and by the multi-stakeholder Internet governance community.



Jon Postel (L) started the IANA; with Steve Crocker and Vint Cerf (R)



Let's drill down into some areas of IANA operations

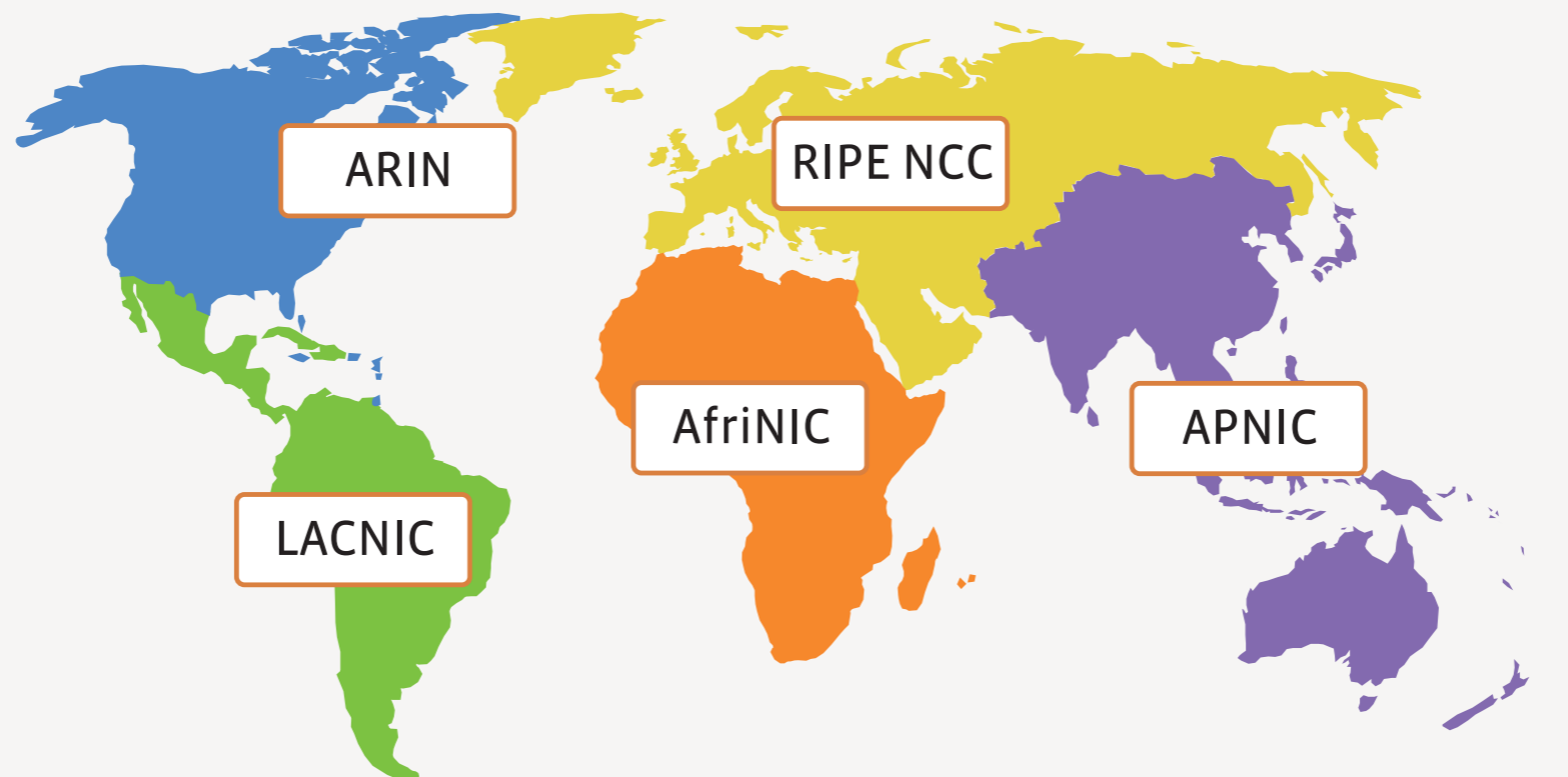
- Learn about the role of **Regional Internet Registries**
- How **country-code TLDs** are managed
- How **internationalization** works with domain names
- The utility of **key signing ceremonies**
- How **time zones** key the world synchronized

Number Resources and the RIRs



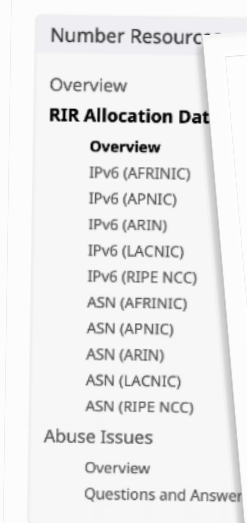
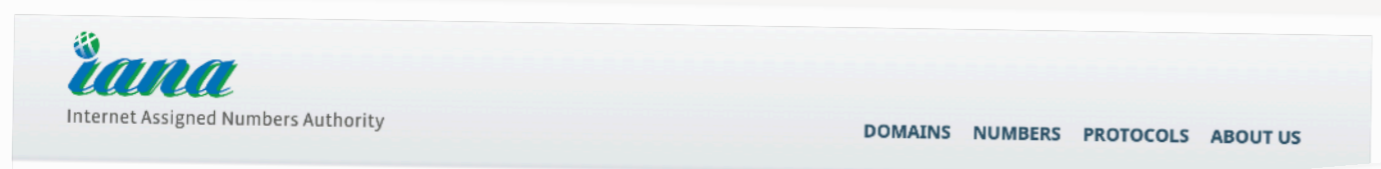
Number Allocation

- ▶ While IANA is responsible for the entire address space of these identifiers, customers who need general-use IP addresses and AS numbers do not come directly to IANA.
- ▶ Instead, they are distributed through a regional distribution system involving five **Regional Internet Registries**



Allocation of Number Resources by IANA

- IANA allocates large blocks of IP addresses and ASNs to the five RIRs
 - These allocations are made according to global policies, established by ICANN's Address Supporting Organization (ASO)
- Allocations are made in compliance with service level agreements (SLAs) defined in the Service Level Agreement for the IANA Numbering Services
- Deterministic decision making is used, using formulas to identify when RIRs qualify for more IANA allocations.

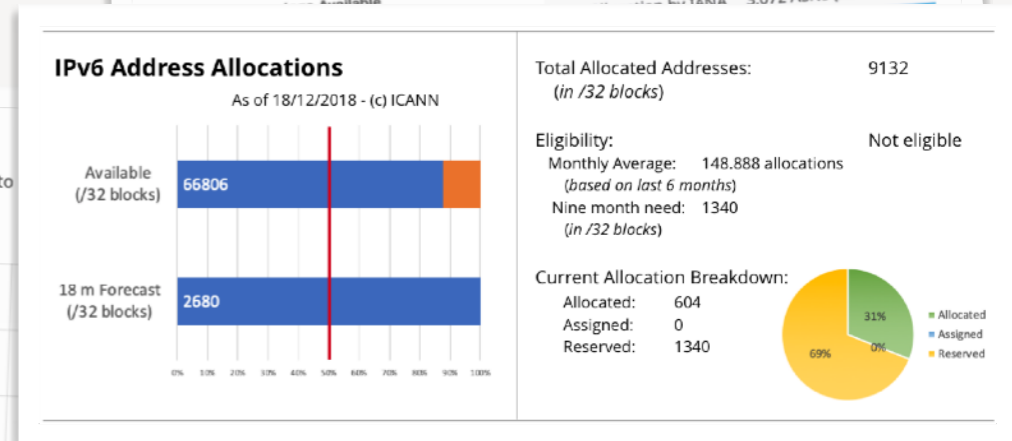
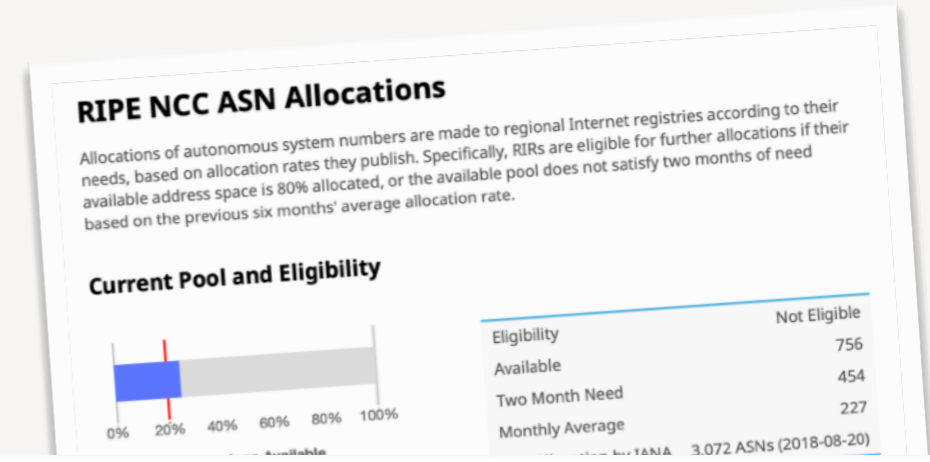
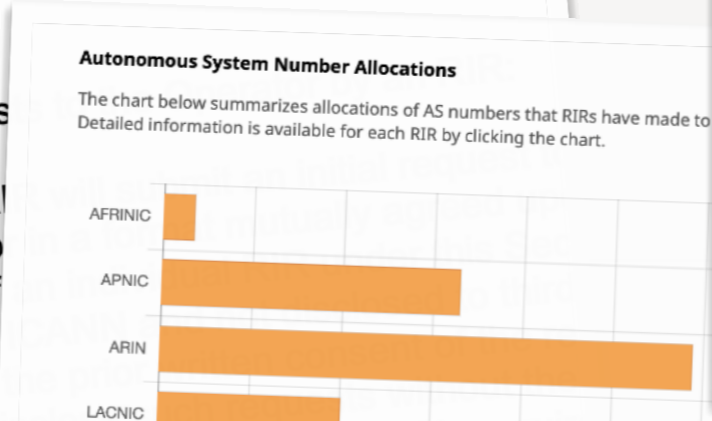


4.3 IANA Numbering Service Operational Requirements

The Operator shall perform the IANA Numbering Service in accordance with the following requirements:

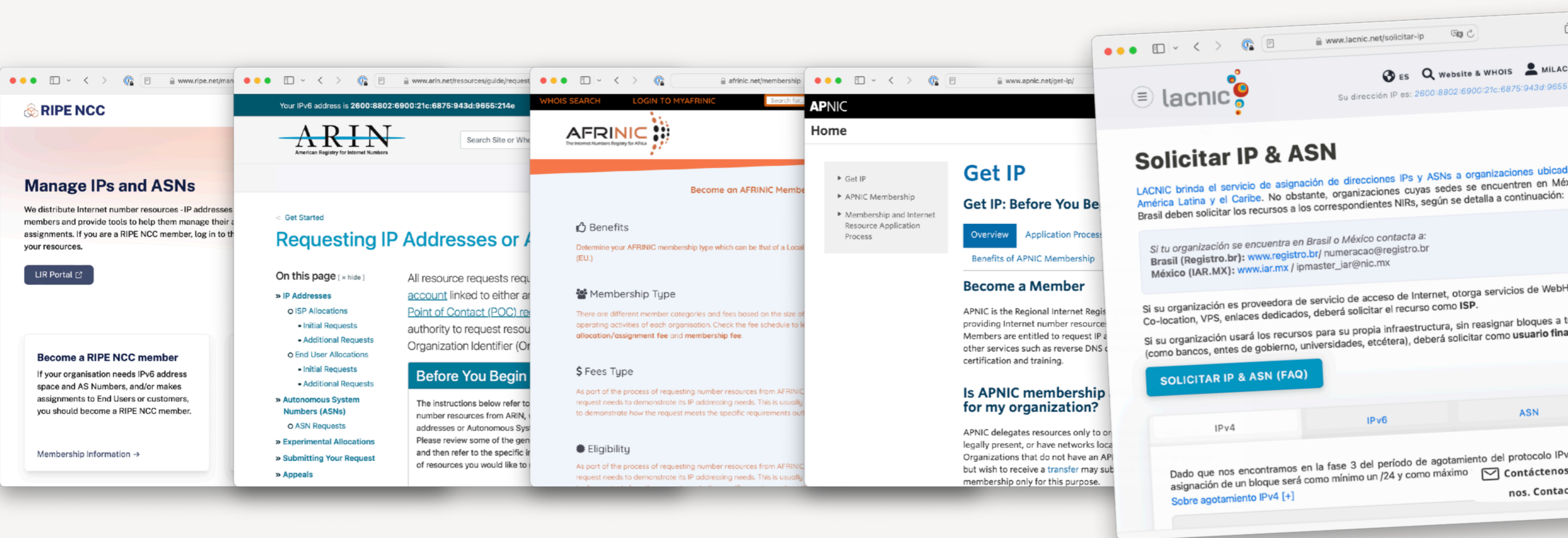
Process for handling of requests:

- (a) A requesting RIR shall submit a request by email (e-mail), or by other means of communication, to the IANA Numbering Service with confidence by the IANA Numbering Service (RIRs) without



Allocation of Number Resources by RIRs

- Each RIR operates in its own service region, and sets policies through its own communities and accountability mechanisms.
- Periodical conferences and policy development apparatus
- Similar to ICANN, but at a regional-level for number resources
- Network operators apply for resources in their respective region



Country-code top-level domains (ccTLDs)

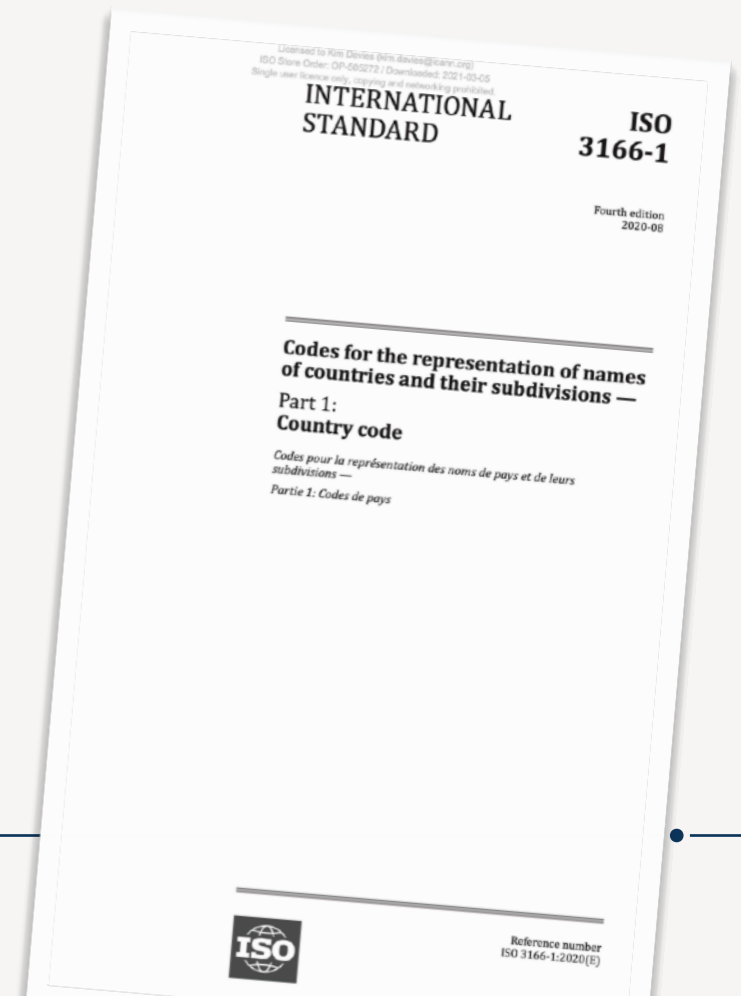
A scenic landscape at dusk or dawn. The sky is a deep blue with scattered clouds, transitioning to a soft pink and orange glow near the horizon. In the foreground, there is a body of water reflecting the sky. A small, dark island is visible in the middle ground, and a large, dark hillside rises on the right side of the frame. The overall mood is serene and atmospheric.

What are ccTLDs?

- We typically divide top-level domains into two broad categories:
 - **Generic Top-Level Domains (gTLDs)**
 - Global purpose
 - ICANN policy making and oversight
 - **Country-code Top-Level Domains (ccTLDs)**
 - Country-level purpose
 - Local policy making and oversight (within country)
 - Automatic qualification/disqualification
- Policy that applies at the global level is devised within two respective ICANN supporting organizations: the GNSO and ccNSO respectively.
- The enduring principles that define a ccTLD are contained in a seminal document “RFC 1591”, published in 1994 by Jon Postel

Country-code Top-Level Domains

- As the name implies, derived not from countries but from **country codes**
 - Country codes are specified by the international standard ISO 3166-1
 - This standard is used for many applications, not just ccTLDs (e.g. passports, currency, postal mail, even language subtags discussed earlier)
 - It provides alphabetical and numerical codings for countries and territories, ccTLDs only use one kind of coding — alpha-2 (two letters)
 - It is both the arbiter of
 - (a) what country/territory is eligible, and
 - (b) what their code should be, based on the notion such decisions shouldn't be done by IANA.



ISO 3166-1 alpha-2 codes

AA	BA	CA	DA	EA	FA	GA	HA	IA	JA	KA	LA	MA	NA	OA	PA	QA	RA	SA	TA	UA	VA	WA	XA	YA	ZA
AB	BB	CB	DB	EB	FB	GB	HB	IB	JB	KB	LB	MB	NB	OB	PB	QB	RB	SB	TB	UB	VB	WB	XB	YB	ZB
AC	BC	CC	DC	EC	FC	GC	HC	IC	JC	KC	LC	MC	NC	OC	PC	QC	RC	SC	TC	UC	VC	WC	XC	YC	ZC
AD	BD	CD	DD	ED	FD	GD	HD	ID	JD	KD	LD	MD	ND	OD	PD	QD	RD	SD	TD	UD	VD	WD	XD	YD	ZD
AE	BE	CE	DE	EE	FE	GE	HE	IE	JE	KE	LE	ME	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE	YE	ZE
AF	BF	CF	DF	EF	FF	GF	HF	IF	JF	KF	LF	MF	NF	OF	PF	QF	RF	SF	TF	UF	VF	WF	XF	YF	ZF
AG	BG	CG	DG	EG	FG	GG	HG	IG	JG	KG	LG	MG	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	ZG
AH	BH	CH	DH	EH	FH	GH	HH	IH	JH	KH	LH	MH	NH	OH	PH	QH	RH	SH	TH	UH	VH	WH	XH	YH	ZH
AI	BI	CI	DI	EI	FI	GI	HI	II	JI	KI	LI	MI	NI	OI	PI	QI	RI	SI	TI	UI	VI	WI	XI	YI	ZI
AJ	BJ	CJ	DJ	EJ	FJ	GJ	HJ	IJ	JJ	KJ	LJ	MJ	NJ	OJ	PJ	QJ	RJ	SJ	TJ	UJ	VJ	WJ	XJ	YJ	ZJ
AK	BK	CK	DK	EK	FK	GK	HK	IK	JK	KK	LK	MK	NK	OK	PK	QK	RK	SK	TK	UK	VK	WK	XK	YK	ZK
AL	BL	CL	DL	EL	FL	GL	HL	IL	JL	KL	LL	ML	NL	OL	PL	QL	RL	SL	TL	UL	VL	WL	XL	YL	ZL
AM	BM	CM	DM	EM	FM	GM	HM	IM	JM	KM	LM	MM	NM	OM	PM	QM	RM	SM	TM	UM	VM	WM	XM	YM	ZM
AN	BN	CN	DN	EN	FN	GN	HN	IN	JN	KN	LN	MN	NN	ON	PN	QN	RN	SN	TN	UN	VN	WN	XN	YN	ZN
AO	BO	CO	DO	EO	FO	GO	HO	IO	JO	KO	LO	MO	NO	OO	PO	QO	RO	SO	TO	UO	VO	WO	XO	YO	ZO
AP	BP	CP	DP	EP	FP	GP	HP	IP	JP	KP	LP	MP	NP	OP	PP	QP	RP	SP	TP	UP	VP	WP	XP	YP	ZP
AQ	BQ	CQ	DQ	EQ	FQ	GQ	HQ	IQ	JQ	KQ	LQ	MQ	NQ	OQ	PQ	QQ	RQ	SQ	TQ	UQ	VQ	WQ	XQ	YQ	ZQ
AR	BR	CR	DR	ER	FR	GR	HR	IR	JR	KR	LR	MR	NR	OR	PR	QR	RR	SR	TR	UR	VR	WR	XR	YR	ZR
AS	BS	CS	DS	ES	FS	GS	HS	IS	JS	KS	LS	MS	NS	OS	PS	QS	RS	SS	TS	US	VS	WS	XS	YS	ZS
AT	BT	CT	DT	ET	FT	GT	HT	IT	JT	KT	LT	MT	NT	OT	PT	QT	RT	ST	TT	UT	VT	WT	XT	YT	ZT
AU	BU	CU	DU	EU	FU	GU	HU	IU	JU	KU	LU	MU	NU	OU	PU	QU	RU	SU	TU	UU	VU	WU	XU	YU	ZU
AV	BV	CV	DV	EV	FV	GV	HV	IV	JV	KV	LV	MV	NV	OV	PV	QV	RV	SV	TV	UV	VV	WV	XV	YV	ZV
AW	BW	CW	DW	EW	FW	GW	HW	IW	JW	KW	LW	MW	NW	OW	PW	QW	RW	SW	TW	UW	VW	WW	XW	YW	ZW
AX	BX	CX	DX	EX	FX	GX	HX	IX	JX	KX	LX	MX	NX	OX	PX	QX	RX	SX	TX	UX	VX	WX	XX	YX	ZX
AY	BY	CY	DY	EY	FY	GY	HY	IY	JY	KY	LY	MY	NY	OY	PY	QY	RY	SY	TY	UY	VY	WY	XY	YY	ZY
AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ	KZ	LZ	MZ	NZ	OZ	PZ	QZ	RZ	SZ	TZ	UZ	VZ	WZ	XZ	YZ	ZZ

ISO 3166-1 Codes

AA Assigned in ISO 3166-1 standard

ISO 3166 MA Statuses

AA Transitionally Reserved

AA Exceptionally Reserved

AA Indeterminately Reserved

How are ccTLDs managed?

- ccTLDs are intended to be managed within their respective jurisdiction
 - An appointed trustee (the “ccTLD Manager”) is responsible for all facets of ccTLD operation within the country
 - Local accountability
- IANA is responsible for evaluating requests to manage ccTLDs
 - Evaluates such requests on a number of policy criteria
 - Proceeds with requests when they satisfy all relevant criteria
 - Maintains an ongoing day-to-day operational relationship with the ccTLD manager to ensure the TLD continues to function (managing relevant data in the DNS root zone to enable the TLD)
 - Is not involved in day-to-day administration at the lower level (managing second-level registrations)

Policy responsibilities of ccTLD managers

- “trustees for the delegated domain, and have a **duty to serve the community**” ... “both the nation, in the case of a country code, and the global Internet community”
- “Concerns about ‘rights’ and ‘ownership’ of domains are inappropriate. ... be concerned about **‘responsibilities’ and ‘service’ to the community.**”
- **“equitable to all groups”**
- **“Significantly interested parties** in the domain should agree [the ccTLD manager]”
- “actual management of the assigning of domain names, delegating subdomains and operating nameservers must be **done with technical competence**”
- “This includes keeping [IANA] advised of the status of the domain, **responding to requests in a timely manner**, and operating the database with **accuracy, robustness, and resilience**”

Internationalized Domain Names (IDNs)

A scenic landscape at dusk or dawn. The sky is a deep blue with scattered white clouds. The horizon shows a soft pink and orange glow. In the foreground, there is a body of water reflecting the sky. A dark, silhouetted hillside is visible on the right, and a small island or headland is in the middle ground.

grancompania.co

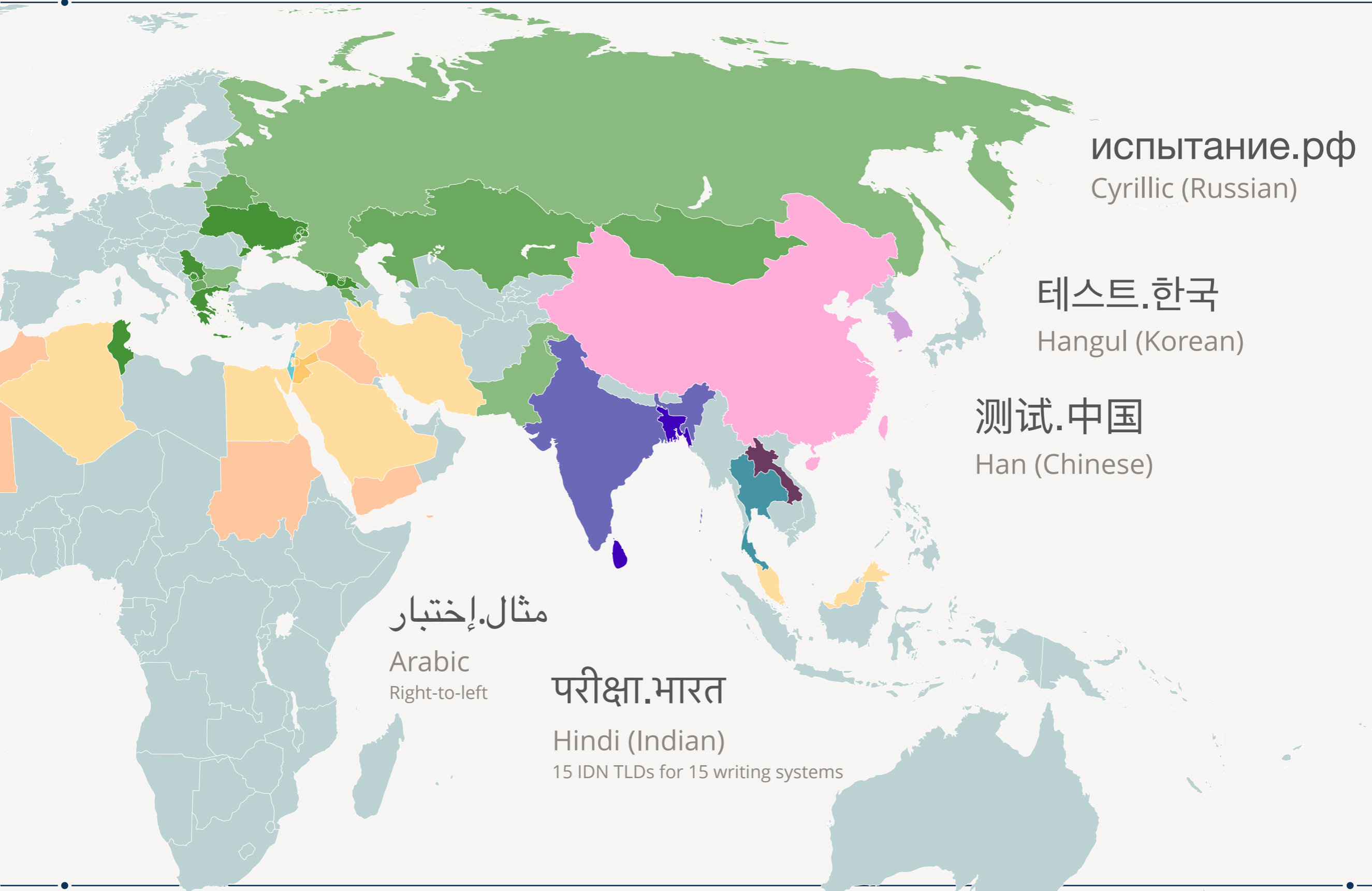
- Letters a-z
- Digits 0-9
- Hyphens

grancompania.co

grancompañía.co

- Expressive beyond just what is provided by the ASCII (English) alphabet

Really useful for non-Latin scripts



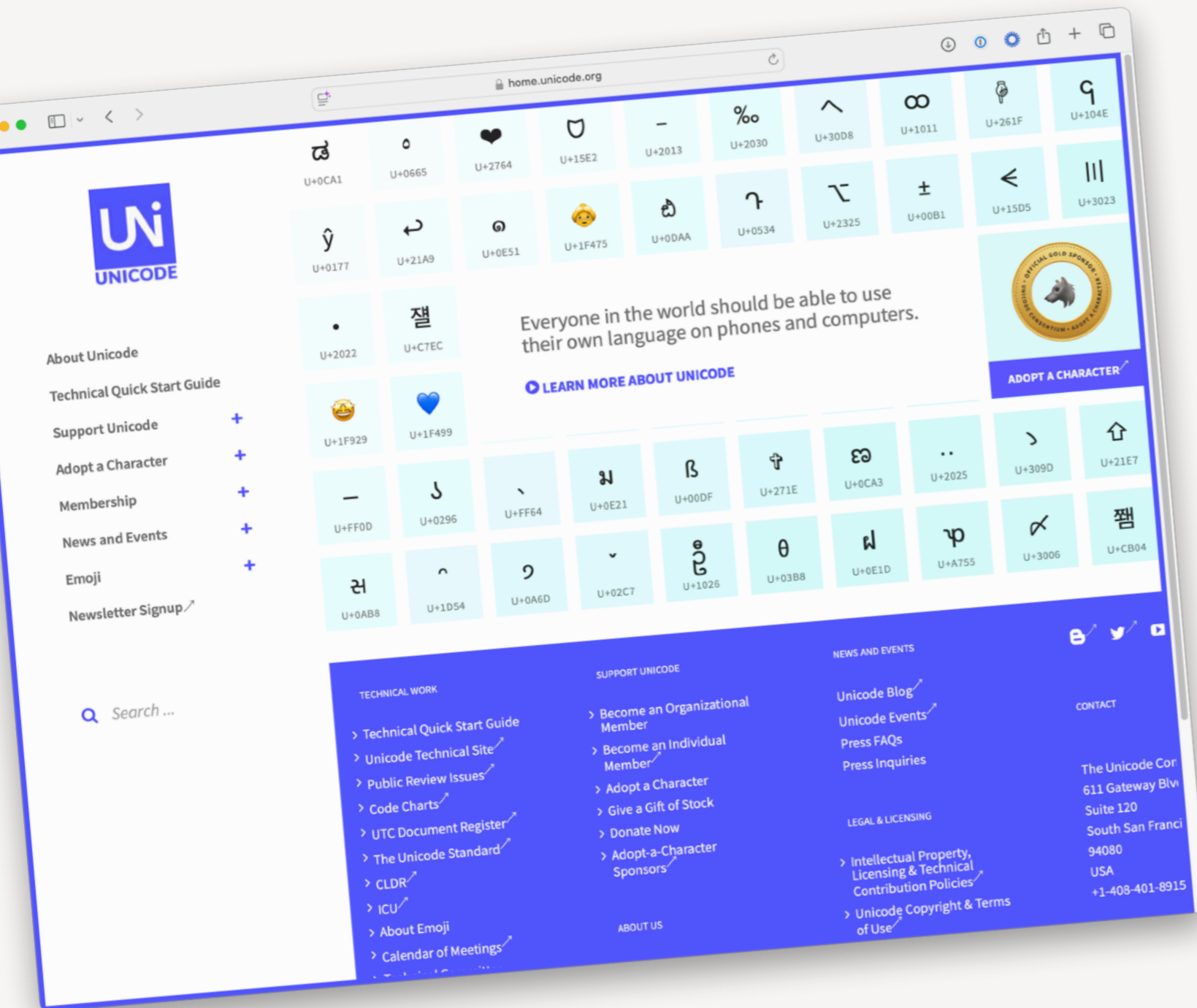
grancompañía.co



xn--grancompaa-s8a1c.co

- Internally, still comprised of letters-digits-hyphens
- Algorithm converts between two representations

Based on Unicode



- 154,998 characters
- 37 in LDH
- Aims to encapsulate all the world's writing systems

Unicode brings challenges


- So many letters in different writing systems look alike or are confusable
- Unicode encapsulates symbols and other elements used in written communication
- IDNA standard limits Unicode to only those that represent “letters” or letter-like things, no symbols or punctuation
- Special characters for things like joining have specific limited rules on where they can appear
- Much like the original LDH rules, constrains the possibilities to a reasonable subset
- Doesn’t solve all the problems — mitigating the issues requires domain registries to implement specific rules for specific languages, formerly known as “IDN tables”, now “Label Generation Rulesets”

Label Generation Rulesets

- Rules that govern which letters and characters are needed to represent specific languages
- You cannot commingle letters between languages to avoid confusability
- Context rules where they can be constructed
- Sets of code points that are interchangeable bundled together in “variant sets”

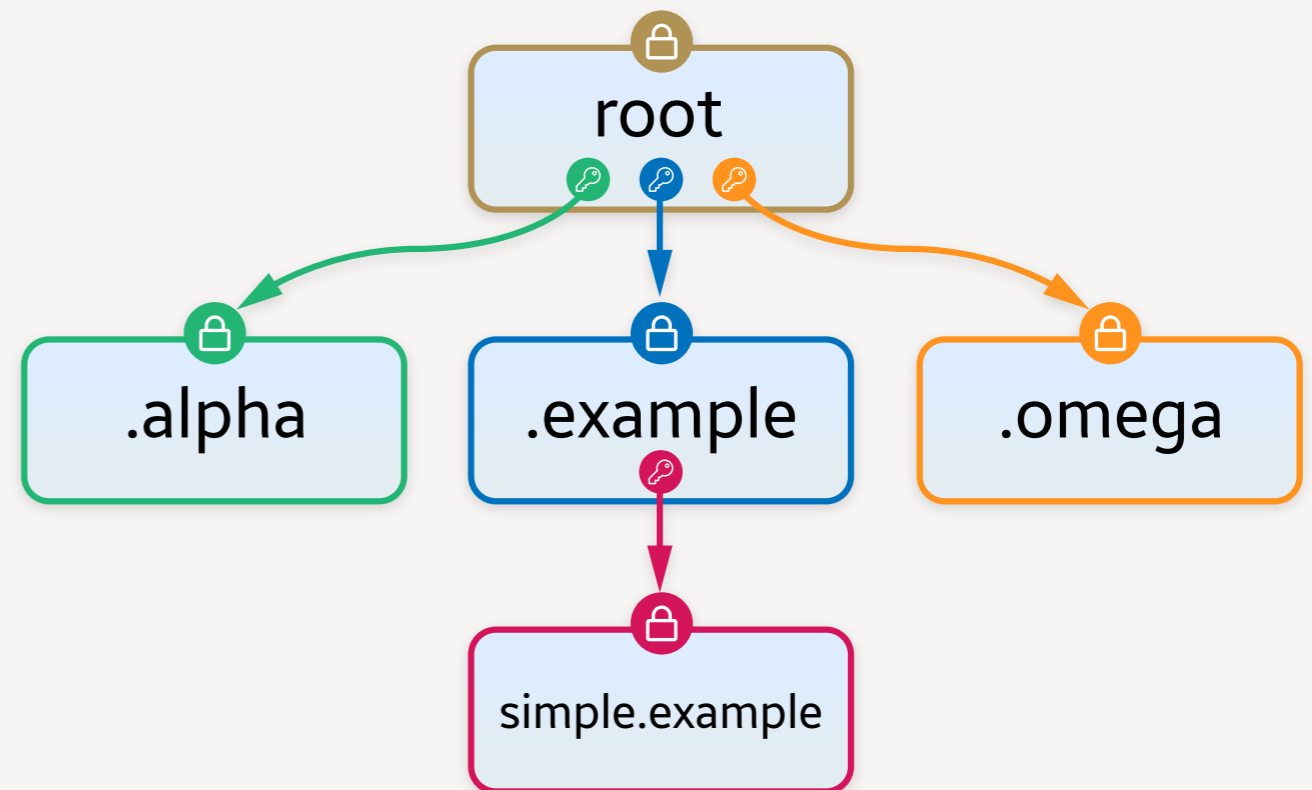
- IANA developed the technical standard (RFC 7940), and houses a global repository of these rulesets contributed by TLD registries
- ICANN has expert panels that develops common rules to be used at the root zone and to harmonize across different domains

DNS Security and Key Signing Ceremonies

A scenic landscape at dusk or dawn. The sky is a deep blue with scattered clouds, transitioning to a soft pink and orange glow near the horizon. In the foreground, there is a body of water reflecting the sky. A small, dark island is visible in the middle ground, and a large, dark hillside rises on the right side of the frame. The overall mood is serene and quiet.

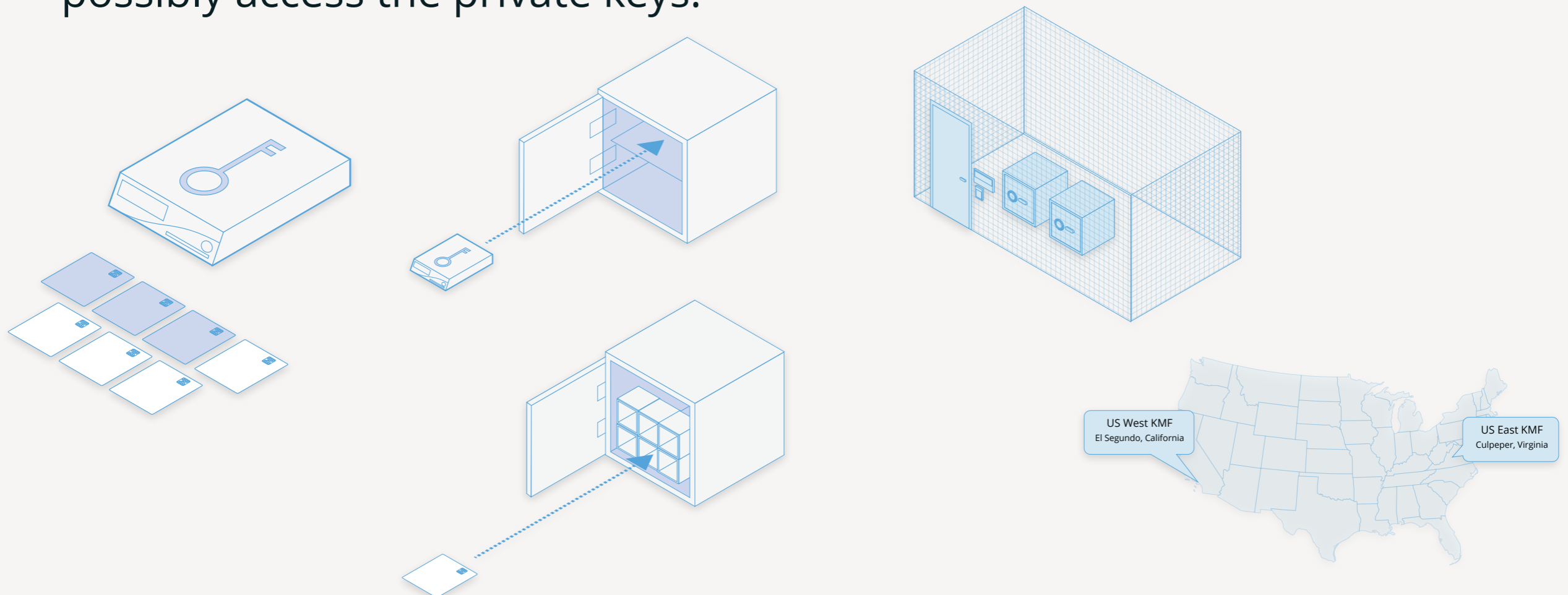
DNS Trust Anchor

- Security for the DNS (DNSSEC) is a hierarchical system of public key cryptography that matches the hierarchical delegation of the DNS itself.
- The apex key is the **Root Zone Key Signing Key (KSK)**, which serves as the singular trust anchor for the system.
- In association with its role in managing the DNS root zone, IANA also manages the Root Zone KSK.



Key ceremonies

- Approximately four times a year, special events are held called key signing ceremonies. During these events, specialized equipment is used to generate the cryptographic signatures required to secure the DNS root zone.
- Access and roles are split among many people, so no one person can possibly access the private keys.



Key ceremonies

- Each ceremony is orchestrated using a comprehensive script that identifies each individual step that needs to be undertaken.

Act 1: Initiate Ceremony and Retrieve Materials

Open Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
15	CA and IW transport a cart, and escort SSC1 to Tier 5 (Safe Room.)		
16	SSC1 opens Safe #1 while shielding the combination from the camera. <i>Note: SSC will begin by rapidly spinning the dial counter-clockwise in order to charge it.</i>		
17	Perform the following steps to complete the safe log: a) SSC1 removes the existing safe log, then shows the most recent page to the audit camera. b) IW provides the pre-printed safe log to SSC1. c) SSC1 writes the date and time, then signs the safe log where "Open Safe" is indicated. d) IW verifies the entry then initials it.		

Remove Equipment from Safe #1 (Tier 6, Equipment Safe)

Step	Activity	Initials	Time
18	CA performs the following steps to extract each piece of equipment from the safe: a) CAREFULLY remove each equipment TEB from the safe. b) Read aloud each TEB number, then verify its integrity while showing it to the audit camera. c) Place each equipment TEB on the cart as specified on the list below. d) Write the date, time, and signature on the safe log where "Remove" is indicated. e) IW verifies the safe log entry, then initials it. HSM3: TEB # BB51184512 (Place on Cart) HSM4: TEB # BB51184513 (Place on Cart) HSM5W: TEB # BB51184514 (Check and Return) Laptop3: TEB # BB81420125 (Check and Return) Laptop4: TEB # BB81420103 (Place on Cart) OS DVD (release coen-0.4.0) + HSMFD: TEB # BB46584386 (Place on Cart) KSK-2017: TEB # BB46584387 (Check and Return) HSM3 Physical Keyboard Key: TEB # BB21907221 (Place on Cart)		

Close Safe #1 (Tier 6, Equipment Safe) Exit Tier 5 (Safe Room)

Step	Activity	Initials	Time
19	SSC1 writes the date and time, then signs the safe log where Close Safe is indicated. IW verifies the safe log entry then initials it.		
20	SSC1 returns the safe log back to Safe #1, closes the safe door, pulls up on the handle, and ensures it's locked by spinning the dial at least two full revolutions each way, counter-clockwise then clockwise. CA and IW verify that the safe is locked and the "WAIT" light indicator is off.		
21	CA, IW, and SSC1 leave Tier 5 (Safe Room) with the cart, returning to Tier 4 (Key Ceremony Room).		

Root DNSSEC KSK Ceremony 40 Page 8 of 38

Act 3: Activate HSM (Tier 7) and Generate Signatures

Verify the KSR Hash for KSR 2020 Q2

Step	Activity	Initials	Time
8	When the hash of the KSR is displayed on the terminal window, perform the following: a) CA asks the Root Zone Maintainer (RZM) representative to identify themselves in front of the room and provide documents for IW to review off camera for the purpose of authentication. b) IW retains the hash and PGP word list for KSR 2020 Q2, and employment verification letter provided by the RZM representative and writes their name on the following line: _____		
9	c) RZM representative reads aloud the PGP word list SHA-256 hash of the KSR file being used.		
9	Participants confirm that the hash displayed on the terminal window matches with the RZM discourse, then CA asks "are there any objections?"		
10	CA enters "y" in response to "Is this correct (y/N)?" to complete the KSR signing operation. The SKR is located in: <code>/media/KSR/KSR40/skr-root-2020-q2-0.xml</code>		

Print Copies of the KSR Signer log

Step	Activity	Initials	Time
11	CA executes the commands below using the terminal window to print the KSR Signer log: a) <code>lpadmin -p HP -o copies-default=X</code> <i>Note: Replace "X" with the amount of copies needed for the participants.</i> b) <code>printlog^[8] krsigner-202002*.log</code>		
12	IW attaches a copy of the required krsigner log to their script.		

Back up the Newly Created SKR

Step	Activity	Initials	Time
13	CA executes the following commands using the terminal window: a) List the contents of the KSR FD by executing: <code>ls -ltrR /media/KSR</code> b) Copy the contents of the KSR FD to the HSMFD by executing: <code>cp -pR /media/KSR/*</code> <i>Note: Confirm overwrite by entering "y" if prompted.</i> c) List the contents of the HSMFD to verify it has been copied successfully by executing: <code>ls -ltrR</code> d) Unmount the KSR FD by executing: <code>umount /media/KSR</code>		
14	CA removes the KSR FD containing the SKR files, then gives it to the RZM representative.		

Root DNSSEC KSK Ceremony 40 Page 15 of 38

Act 4: Zeroize and Dismantle Hardware Security Module

Remove Cryptographic Module and Card Reader from HSM3

Step	Activity	Initials	Time
15	CA performs the following steps to remove the cryptographic module: a) Using Tool A+Bit 4 , remove the 4 nuts which secure the cryptographic module to the case. b) Lift the cryptographic module up to separate it from the case. c) Using Tool C , remove both connectors from the cryptographic module as flush with the case as possible. d) Place the cryptographic module in the Critical Parts bin, and the connectors in the HSM Parts bin on the ceremony table.		
16	CA performs the following steps to remove the front panel and card reader: a) Using Tool A+Bit 4 , remove the 4 nuts which secure the front panel to the bottom of the case. b) Place the front panel in the HSM Parts bin on the ceremony table. c) Using Tool A+Bit 4 , remove the nut which secures the card reader. d) Using Tool A+Bit 3 , remove the 3 screws which secure the card reader. e) Lift the card reader up to separate it from the case and place it with the ribbon cable in the Critical Parts bin on the ceremony table. f) Place the HSM case in the HSM Parts bin on the ceremony table.		

Place the Critical HSM3 parts into a TEB

Step	Activity	Initials	Time
17	CA places the container with the following critical parts into a prepared TEB, then seals it. a) Cryptographic Module b) Logic Board c) Card Reader <i>Note: The HSM case will not be destroyed.</i>		
18	CA performs the following steps: a) Read aloud the TEB number, then show it to the audit camera above for participants to see. b) Confirm with IW that the TEB number matches below. c) Initial the TEB along with IW using a ballpoint pen. d) Give IW the sealing strips for post-ceremony inventory. e) Give RKOS the TEB for destruction. HSM3: TEB # BB81420112		

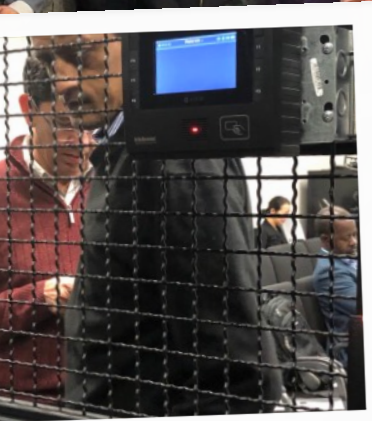
Retire HSM Physical Keyboard Key

Step	Activity	Initials	Time
19	CA performs the following steps to retire the listed HSM Physical Keyboard Key: a) Remove the TEB from the cart. b) Inspect TEB for tamper evidence. c) Read aloud the TEB number while IW verifies the information using the previous ceremony script where it was last used. d) Remove and discard the TEB. e) RKOS will take possession of the HSM Physical Keyboard Key and place in its designated area. HSM3 Physical Keyboard Key: TEB # BB21907221 Last Verified: AT22 2015-07-20		

Root DNSSEC KSK Ceremony 40 Page 23 of 38

Trusted Community Representatives

- We use **trusted community representatives**, security experts from around the world, in many of the critical roles in the ceremony.
- Current and former Latin American and Caribbean participants:
 - Hugo Salgado, Carlos Martinez, Jorge Etges, Sebastian Castro, Nicolas Antoniello
- New volunteers welcome at <https://iana.org/tcr>



- Beyond in person attendance, ceremonies are streamed online and media is often in attendance to explain the story.
- The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the KSK has not been compromised.

Root KSK Ceremony 33
663 views

15 likes, 0 dislikes, SHARE, ...

Top chat replay

- Antranig Vartanian thanks for the reply!
- Internet Assigned Numbers Authority Make sense? Any other questions about this discrepancy?
- Kim Davies The script is pre-populated with serial numbers on the bags as a convenience (w used to write them in manually during the ceremony). In this case it looks like there was an error ...
- Kim Davies ... in that the wrong serial number was placed in the pre-printed field. There was no gap in the bag's custody and the serial number of the bag is correct.
- Internet Assigned Numbers Authority Materials from previous ceremonies can be found at <http://ta.iana.org/ksk-ceremony/>
- Internet Assigned Numbers Authority The bags set for ceremony 31 were never used so the serial number from ceremony 29 is what was found.
- Internet Assigned Numbers Authority *some of the bags were not used due to last minute cancellations
- Dev Anand Teelucksingh Thanks for this. So are the bag serial numbers (even temporary ones that may not be used) recorded in previous KSK scripts?
- Dev Anand Teelucksingh Thanks for the prompt replies

Root KSK Ceremony 34

This DNSSEC key signing ceremony is planned for 15 August 2018, 2000 UTC

Location	Root Zone Key Management Facility West El Segundo, California, USA
Ceremony Start	2018-08-15 20:00:00 UTC Wednesday 15 August 2018, 1 p.m. (local time at facility)
Objectives	Sign the ZSK for 2018Q4

Observing the ceremony

The key signing ceremony is a public event, and you are welcome to observe. Only a small number of persons are able to participate as observers at a ceremony broadcast ceremonies as they happen, and will provide recordings after the ceremony. Prior to observing a ceremony, we recommend you review the ceremony materials in advance.

Keeping the world on time

Time Zones

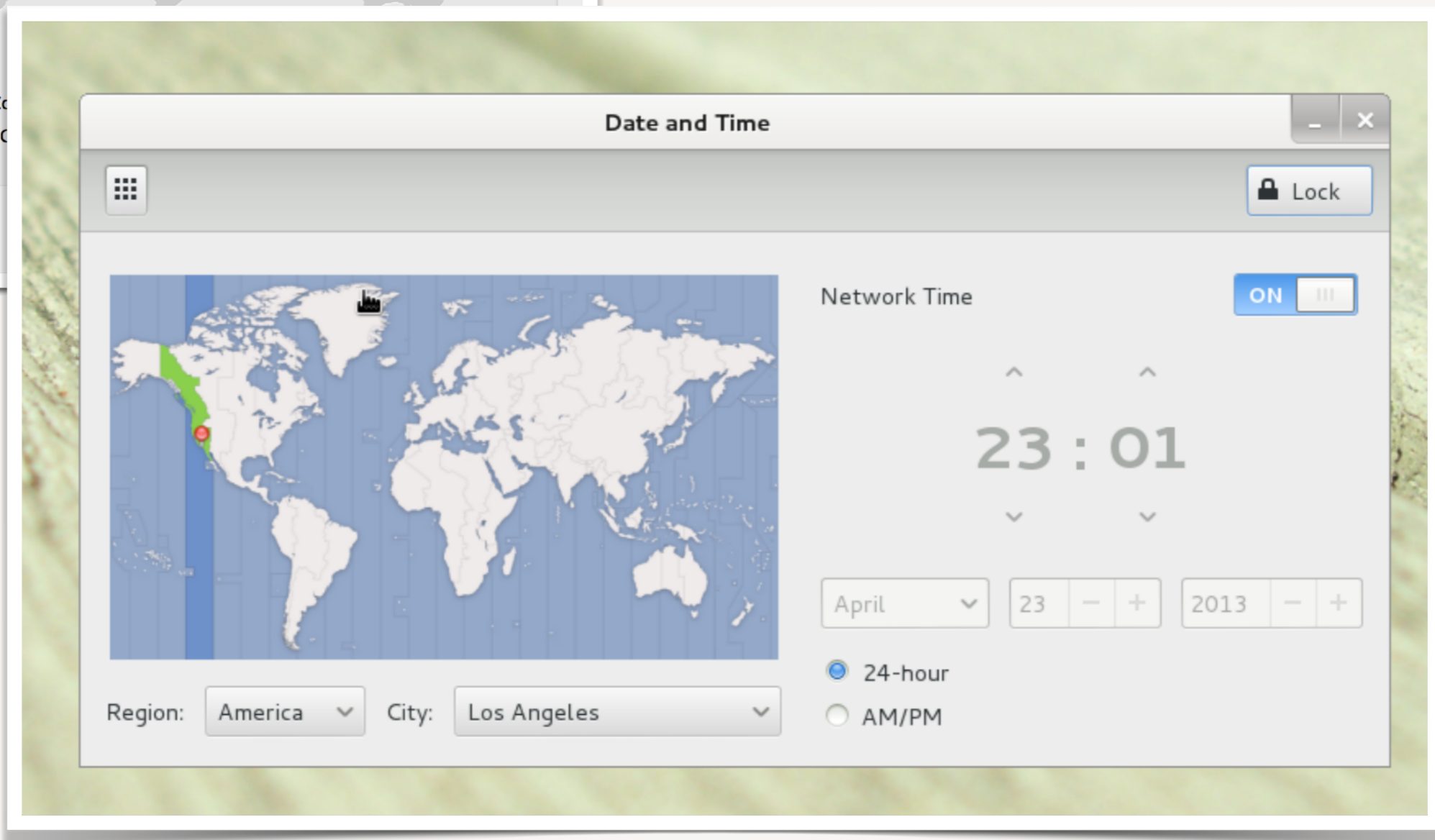
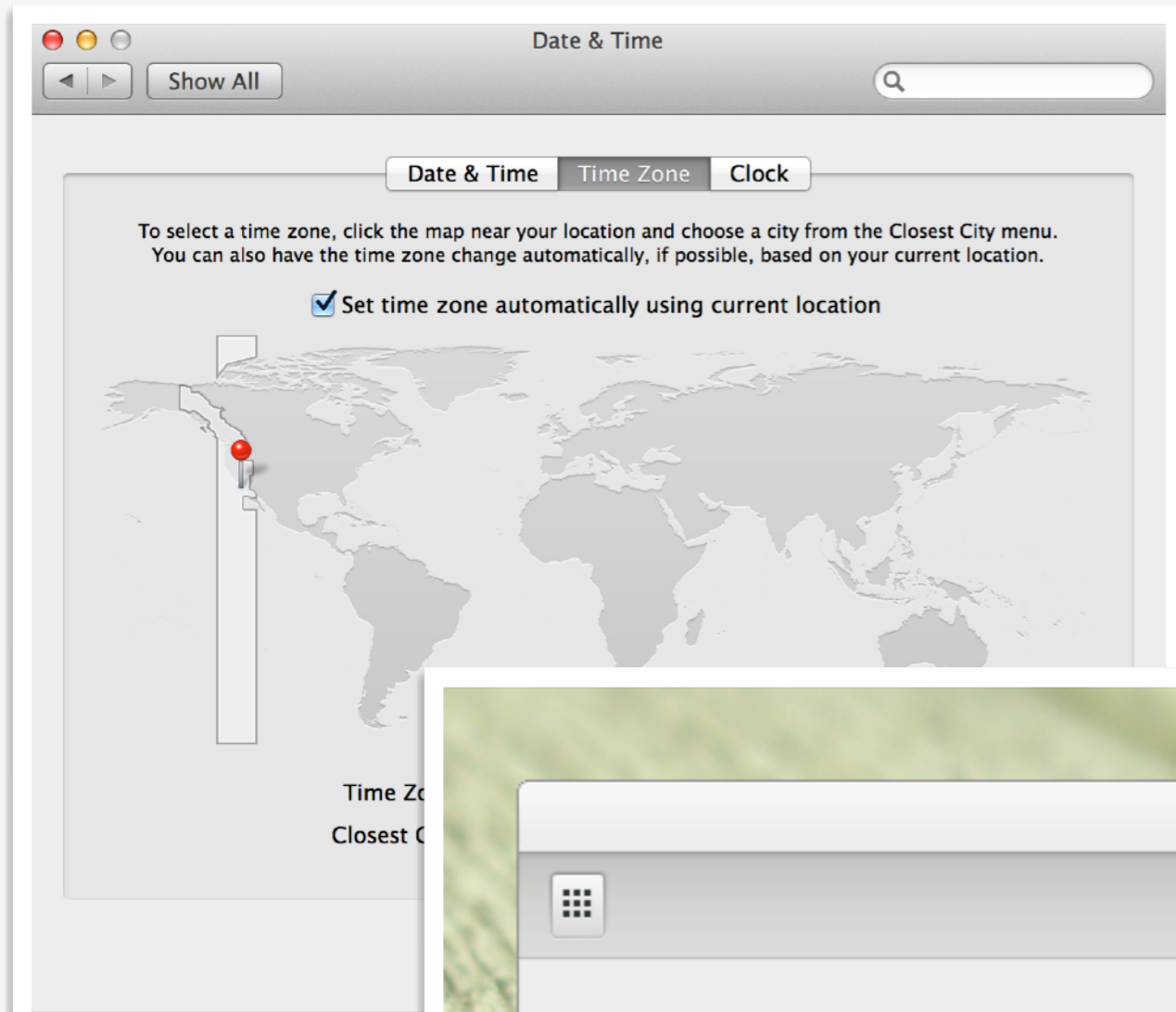
- In the past...
 - Time was calculated based in each locality based on the average of when the sun was at its highest being midday (**local mean time**).
 - Zero longitude, through Greenwich Observatory in London, became a reference point for others in this system (**Greenwich mean time**, or GMT)
 - For each degree of longitude, add/subtract 4 minutes
 - This was fine until consistency of time across multiple locations became a factor
 - Railway timetables motivated in moving beyond this system, railroad companies implemented the timezones we know today in 1883.
 - US Congress adopted the railroad's system as official US time in 1918.

Time Zones

- In modern era...
 - The time in a location is derived from a constant global source of time known as **Coordinated Universal Time** (UTC)
 - Rather than fractional offsets based on longitude of individual places, large bands of '**time zones**' mostly correlate to whole hour offsets
 - A few exceptions (e.g. Nepal is +5:45)
 - In World War I, the idea of shifting the time to promote daylight in the evenings was established in many locations (**daylight saving time**)
 - Used in the summer time when the sun rising early was not seen as advantageous

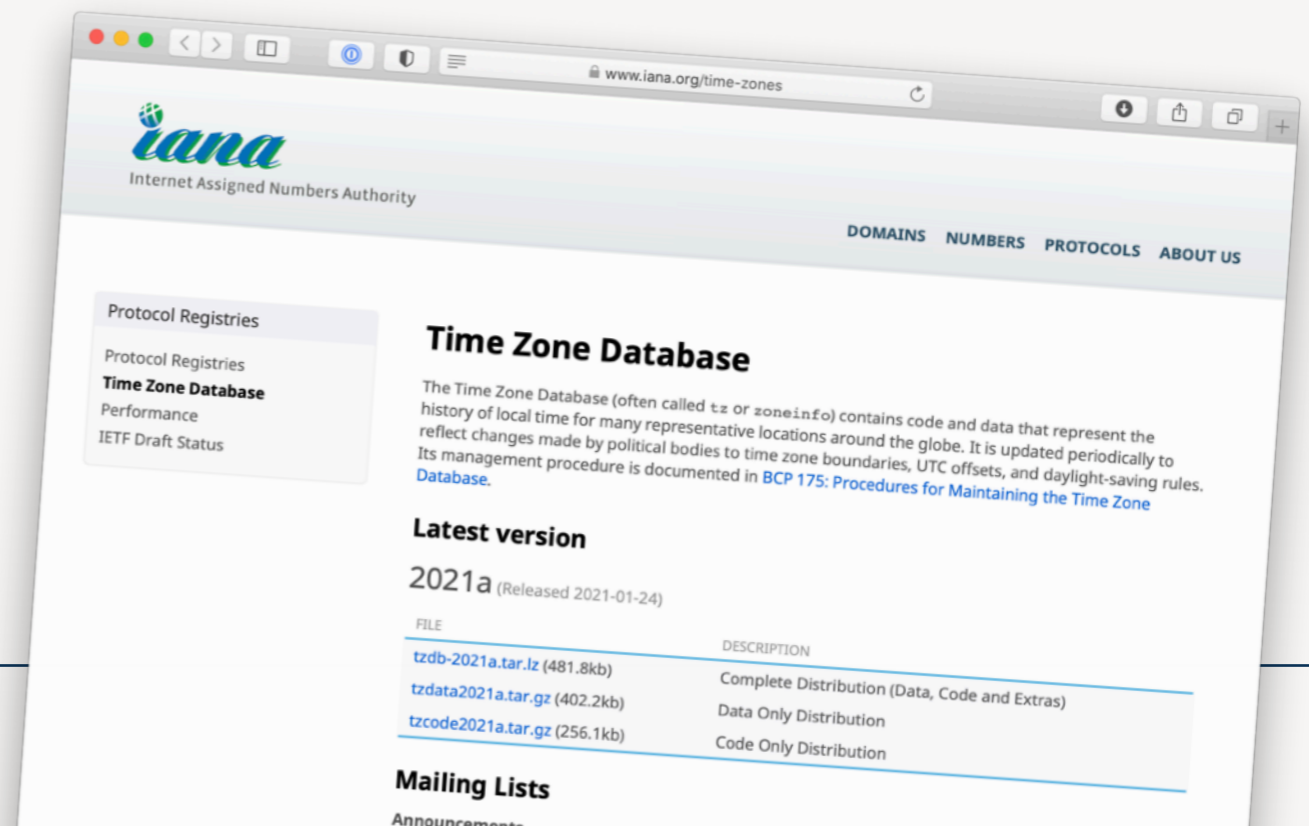
Time Zones

- On computers and devices on the Internet...
 - Computer devices generally store time in UTC, and use special protocols to sync over the Internet to keep time in sync with millisecond precision (NTP)
 - Specialized clocks, like atomic clocks, are used as a reference for NTP servers
 - UTC is good for computers who need consistent record keeping, but doesn't help when you want something to happen at '4pm'



The Time Zone Database

- A public resource, hosted by IANA, that provides data that can help people configure automated time conversations on their devices.
- Not intended for end-user consumption, provides data that is imported into software libraries to implement automated conversions
- Contains:
 - Machine-readable descriptions of time zone offsets, and when offsets change based on time/date (to implement DST)
 - Unique identifiers for each of these rulesets, with names based on a population center



```

1423 # DECRETO 267 DE 1993
1424 # https://www.suin-juriscal.gov.co/viewDocument.asp?ruta=Decretos/1061335
1425
1426 # Rule NAME FROM TO - IN ON AT SAVE LETTER/S
1427 Rule CO 1992 only - May 3 0:00 1:00 -
1428 Rule CO 1993 only - Feb 6 24:00 0 -
1429 # Zone NAME STD OFF RULES FORMAT [UNTIL]
1430 #STD OFF -4:56:16.4
1431 Zone America/Bogota -4:56:16 - LMT 1884 Mar 13
1432 -4:56:16 - BMT 1914 Nov 23 # Bogotá Mean Time
1433 -5:00 CO %z

```

1629	# Rule	NAME	FROM	TO	-	IN	ON	AT	SAVE	LETTER/S
1630	Rule	Para	1975	1988	-	Oct	1	0:00	1:00	-
1631	Rule	Para	1975	1978	-	Mar	1	0:00	0	-
1632	Rule	Para	1979	1991	-	Apr	1	0:00	0	-
1633	Rule	Para	1989	only	-	Oct	22	0:00	1:00	-
1634	Rule	Para	1990	only	-	Oct	1	0:00	1:00	-
1635	Rule	Para	1991	only	-	Oct	6	0:00	1:00	-
1636	Rule	Para	1992	only	-	Mar	1	0:00	0	-
1637	Rule	Para	1992	only	-	Oct	5	0:00	1:00	-
1638	Rule	Para	1993	only	-	Mar	31	0:00	0	-
1639	Rule	Para	1993	1995	-	Oct	1	0:00	1:00	-
1640	Rule	Para	1994	1995	-	Feb	lastSun	0:00	0	-
1641	Rule	Para	1996	only	-	Mar	1	0:00	0	-

1657	Rule	Para	1996	2001	-	Oct	Sun>=1	0:00	1:00	-
------	------	------	------	------	---	-----	--------	------	------	---

1659	Rule	Para	1997	only	-	Feb	lastSun	0:00	0	-
------	------	------	------	------	---	-----	---------	------	---	---

1662	Rule	Para	1998	2001	-	Mar	Sun>=1	0:00	0	-
------	------	------	------	------	---	-----	--------	------	---	---

1667	Rule	Para	2002	2004	-	Apr	Sun>=1	0:00	0	-
------	------	------	------	------	---	-----	--------	------	---	---

1668	Rule	Para	2002	2003	-	Sep	Sun>=1	0:00	1:00	-
------	------	------	------	------	---	-----	--------	------	------	---

1677	Rule	Para	2004	2009	-	Oct	Sun>=15	0:00	1:00	-
------	------	------	------	------	---	-----	---------	------	------	---

1678	Rule	Para	2005	2009	-	Mar	Sun>=8	0:00	0	-
------	------	------	------	------	---	-----	--------	------	---	---

1690	Rule	Para	2010	max	-	Oct	Sun>=1	0:00	1:00	-
------	------	------	------	-----	---	-----	--------	------	------	---

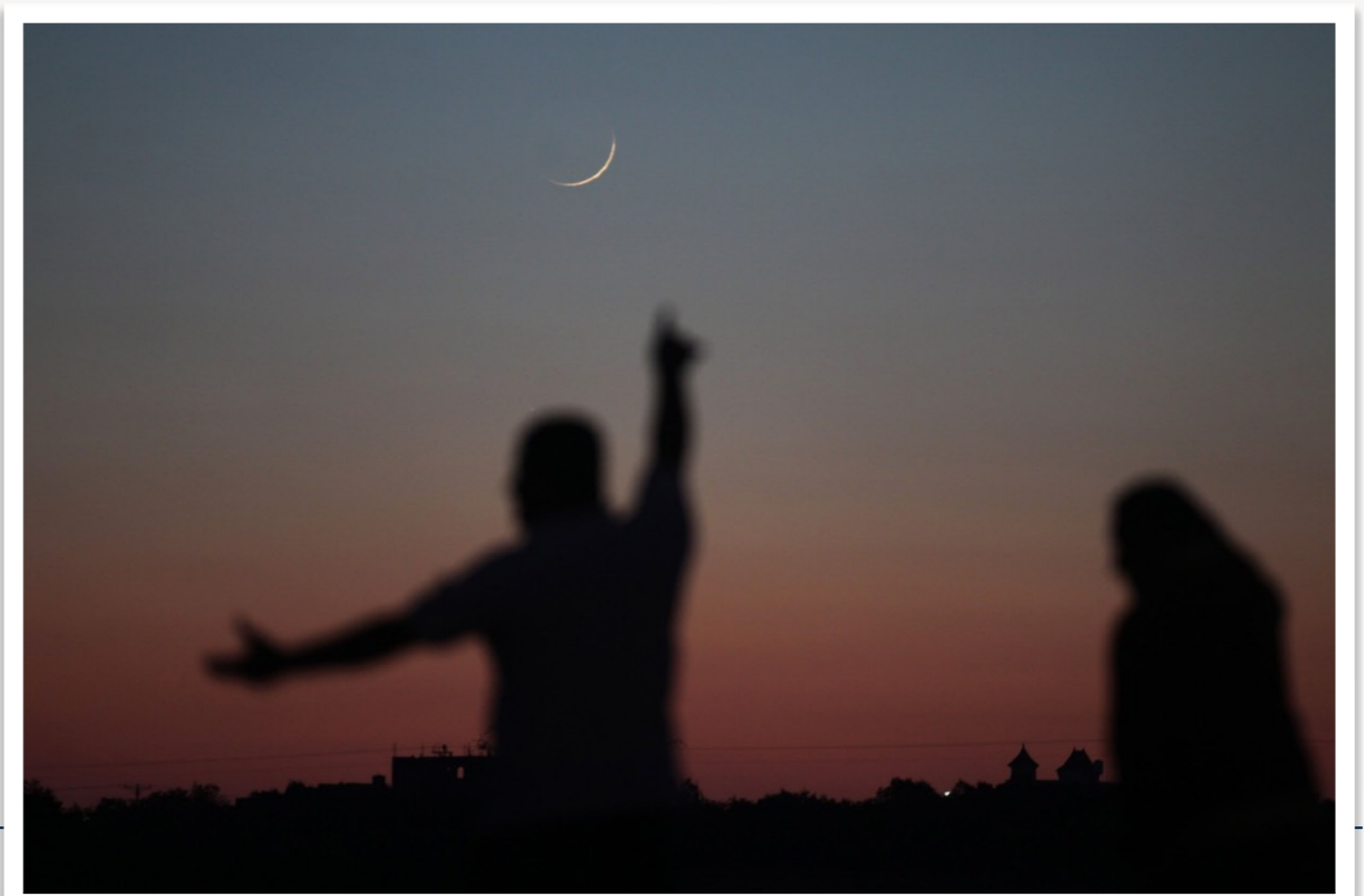
1691	Rule	Para	2010	2012	-	Apr	Sun>=8	0:00	0	-
------	------	------	------	------	---	-----	--------	------	---	---

The Time Zone Database

- It's not official
 - Based on observations on 'facts on the ground'
 - Comprehensive notes in the repository explaining sources
 - Tries to source for authoritative sources (e.g. government laws and decrees)
- Has become the defacto world standard for time zone representation
 - Used in most software, operating systems, etc.

Other interesting time zone facts

- The earth is not spinning at a constant rate, so every six months an assessment is made whether to add or remove an extra second to keep UTC in sync with the earth's rotation (known as a 'leap second')
 - These are also tracked in the Time Zone Database
- Some time zones are assessed on non-deterministic criteria, like when the moon is visible with the naked eye



Thank you!

kim.davies@iana.org